



Petitioner's Demonstratives

Datavant, Inc., *Petitioner*, v. Vigilytics LLC, *Patent Owner*

IPR2024-00226

U.S. Patent No. 9,118,641

February 5, 2025 Oral Hearing



VENABLE_{LLP}

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Datavant Exhibit 1025
Datavant v. Vigilytics
IPR2024-00226



Grounds

Ground 1 – Evenhaim (Claims 1-19)

Ground 2 – Evenhaim and Settimi (Claims 1-19)

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Ground 4 – Dick, Landi, and Murphy (Claims 1-6, 11, 12, and 14-19)

Introduction

Grounds 1 and 2 (Evenhaim and Settimi)

- Both tokenize patient identifiers through similar encryption schemes.
- Settimi provides a centralized data warehouse containing medical records de-identified using encrypted IDs (hash functions) for HIPAA compliance.
- Evenhaim describes searching a database for specific patients.
- Patent Owner's incorrect critique of Evenhaim is rendered moot by Settimi.



Introduction

Grounds 3 and 4 (Dick, Landi, and Murphy)

- Both Dick and Landi describe centralized data warehouses.
- Dick describes searching a database for specific patients.
- Landi provides specifics on using encrypted IDs in place of identifying information for HIPAA compliance in a centralized data warehouse.
- Murphy describes settings minimum patient number requirements to block attacks.

Claim 7

[7.a] A system comprising: an encryption server, having a processor and a memory,

[7.b] for producing a token for each individual included in a group composed of multiple individuals identified in a request for healthcare information that characterizes the group,

[7.c] wherein the identity of the individuals in the group is unattainable from the tokens, each token being associated with a corresponding token in a set of de-identified healthcare data,

[7.d] and each token in the set of de-identified healthcare data being associated with healthcare data for a corresponding individual;

[7.e] a data server for producing the requested healthcare information that characterizes the group

[7.f] by identifying the tokens in the set of de-identified healthcare data and the associated de-identified healthcare data that correspond to the produced tokens,

Claim 7

[7.g] wherein the produced **tokens** and the tokens in the set of de-identified data **are similarly encrypted**,

[7.h] and the produced healthcare information is absent personally identifiable information

[7.i] and has been **produced without the individuals in the group having authorized production** of such healthcare information that characterizes the group; and

[7.j] **providing the produced healthcare information** to report the characteristics of the group composed of multiple individuals

[7.k] **absent authorization** at any time from the individuals in the group of individuals to provide the requested healthcare information.

The '641 Patent: De-Identification

- “Health Insurance Portability and Accountability (HIPAA)” regulations. EX1001, 3:65-4:3.
 - HIPAA typically requires patient authorization or de-identification to release protected health information (PHI). *Id.*
- De-Identification
 - “[R]emoving all personally identifiable information 118 or otherwise transforming the PHI 130 so that it cannot be associated with a particular person.” EX1001, 3:43-48.
 - Tokenization is used to de-identify. EX1001, 4:32-35 (“[T]okens 202 correspond to persons treated by healthcare providers but do not reveal the identities of the treated individuals.”).

The '641 Patent: De-Identification

- Tokenization
 - “[M]ay include encrypting respective data that identifies each individual.” EX1001, 2:37-42.
 - May use “one or more encryption techniques ..., for example hash functions and other methodologies.” EX1001, 5:54-67, 4:41-54.
 - Patent Owner acknowledges that “a hash function” qualifies as a “reproducibly irreversible” token. POR, 7.

The '641 Patent: Centralized Database

- “[D]e-identified data server 318 stores records of de-identified data and corresponding tokens 320 obtained from source sites 138 such as pharmacies, ... Each token obtained from the source sites 138 may have been created using the **same token generator 314** used by the encryption server 312, or using any other means that generates the identical token for the same personally identifiable information.” EX1001, 5:45-53.
- Patent Owner’s expert:
 - “Q And that database has only de-identified data and tokens, correct? A That’s all that’s shown” EX1014, 39:2-12.
 - “Q So that would be ... a centralized warehouse of data that came from the various source sites ...? A Yes.” EX1014, 39:2-12, 20:22-23:13.

The '641 Patent: General Process

- A party sends a request for medical information pertaining to individuals to an encryption server. EX1001, 4:32-33, 5:12-30.
- The encryption server generates a request token for each individual using the same method used to create the tokens in the de-identified data server. EX1001, 2:16-18, 4:32-35, 5:35-67.
- The encryption servers send the tokens to the de-identified data server, which searches for matches. EX1001, 4:37-41, 6:1-4.
- The de-identified data server returns matching health care information. EX1001, 6:62-67, 8:17-31.

The '641 Patent

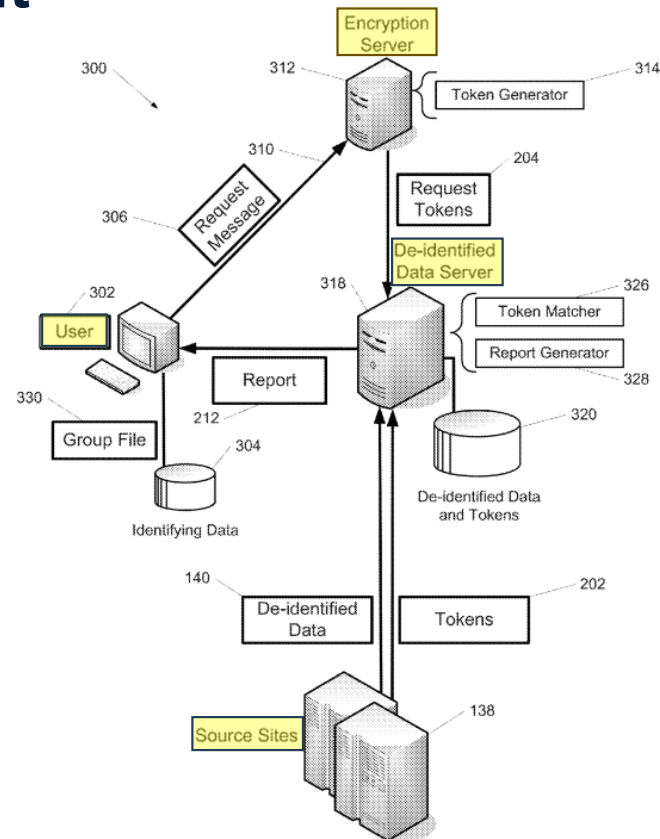


FIG. 3

Reply, 17; POR, 6.

Background: Tokenization

- “The basics of tokenization are straightforward. ... [T]he data is converted into a token which is a globally unique, randomized representation of the real [information].” EX1011, 31.
- Claim Construction
 - Token: “An identifier associated with an individual that does not reveal the identity of the individual.” Pet., 8.

Background: Healthcare Data Searches

Examples

- Pharmaceutical companies looking for patients suited for clinical trials. EX1014, 47:12-50:15.
- Insurance companies looking to determine the risk of insuring a known group of individuals. EX1007, [0003], [0008], [0025], [0037]; EX1001, 1:33-36.
- Medical researchers. EX1006, [0027].

Databases Are Not Limited to One Type of Search

- Patent Owner's expert admitted the same database could be used for various types of searches. EX1014, 47:12-50:15 ("I would assume so.").
 - "The language [in Settimi] says: Medical -- that make medical and/or other products. So that could be – ***that's very broad, I guess.***" EX1014, 102:3-103:8 (EX1006, [0030]).

Background of the Field

HIPAA (45 C.F.R. § 164.514) (Ex2006)

- Expert Determination - “generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.” 164.514(b)(1) (“risk is very small”).
 - “[R]equires removal of PII to the extent that the patient’s identity cannot reasonably be discerned.” Patent Owner Sur-Reply, 3.
- Safe Harbor – Requires removal of specified identifiers. 164.514(b)(2).
- Re-Identification - Permitted, so long as “code or other means of record identification is not derived from or related to information about the individual.” 164.514(c); *see* EX1006 (hashing permitted).

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Evenhaim

- Directed to “compliance with HIPAA.” EX1005, 14:59-67.
- Evenhaim’s “aggregator” accepts user queries for healthcare data concerning a list of specific patients. EX1005, 6:57-67 (“parameter list”).
 - “For example, the instant method can ask about the status of Tom, Dick, Harry, and a further collection of individuals . . . so long as the statistical character of those results will not allow correlation of a result specific back to an individual.” EX1005, 8:18-22.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Evenhaim

- The aggregator sends the query to a “source entity” that holds the healthcare records, which in turn searches for matching records. EX1005, 12:4-13:20.
- Patient identifying information “is replaced with a unique encryption key, such as a one way hash or Advanced Encryption Standard (AES) or the like[.]” EX1005, 12:36-47.
- Evenhaim is intended to improve over systems that provide “physician level behavior.” EX1005, 16:46-57, 7:32-58 (discussing prior systems that “condense their data around large cluster variables—such as by age group”).
 - Evenhaim’s goal: “aggregate the behavior of a group of patients by a pre-defined list of consumers.” EX1005, 16:57-7:3.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Evenhaim

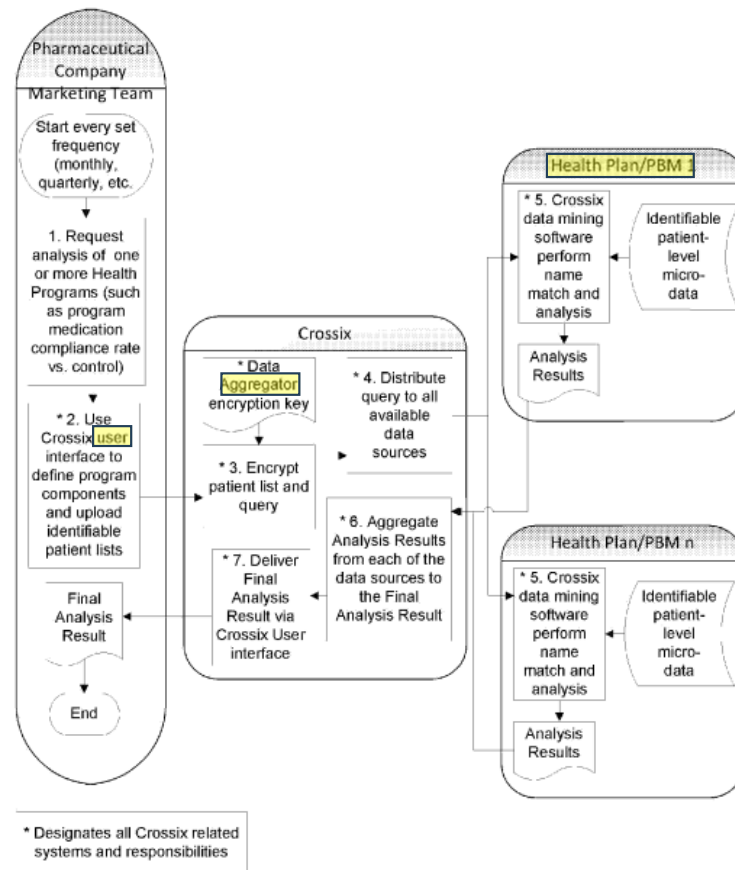


FIG. 4

Pet., 36-39, 41-43

© 2025 / Slide 17

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Patent Owner's Arguments Concerning Evenhaim

- Whether the encryption performed at Evenhaim's aggregator is tokenization (as opposed to standard data transmission encryption).
- Whether the searching at Evenhaim's data source entity is performed by matching encrypted identifiers (tokens), as opposed to decrypting the patient identifiers and searching by name only.

Ground 2's use of Settimi renders these arguments moot.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Combination of Evenhaim and Settimi

- Both use similar encryption schemes to tokenize identifying information.
- The combination uses Settimi's centralized database as the source in Evenhaim's system. Pet., 38-40.
 - Settimi's centralized system allows for one central search in a database that is more robust than prior designs. Pet., 36-37 ("simplified querying").
- Because Settimi's database identifies patient records only by tokens (EPIDs), performing Evenhaim's search for specific patients would involve matching EPIDs, as would be understood by a POSA. Pet., 41-42.
- Both are directed at "reducing the risk of a HIPAA violation." Pet., 37.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Evenhaim's Tokenization

- “[T]here are numerous locations where an encryption of **individual identification** ... could be facilitated. ... [including] on the ‘aggregator’ processor side.” EX1005, 12:24-47 (“identity information ... is replaced with a unique encryption key such as a one way **hash**,” which “preserves the ability to know that two records belong to the same identity”).
- Data transmission encryption vs. parameter list encryption
 - “[T]ransmitting of data ... may preferably include respective encryption and decryption.” EX1005, 13:33-43.
 - “[R]egardless of the general level of encryption elected, a parameter list including ‘individuals’ should carry a stronger level of encryption.” EX1005, 14:3-13.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

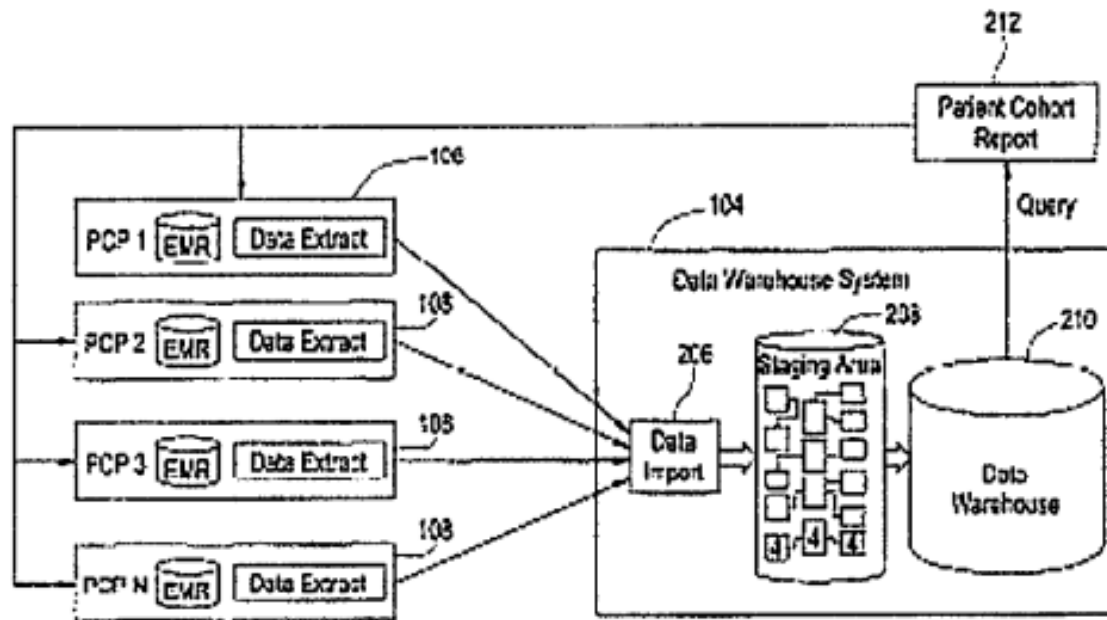
Settimi's Centralized Database of Healthcare Information

- “[A] secure process for sending **de-identified patient information** from a[] patient care provider (PCP) site to a **data warehouse system** where the patient data may be analyzed and compared with a wider range of patient data.” EX1006, [0027].
- “The de-identified patient data is then staged into a data warehouse 210 where it is **available for querying**.” EX1006, [0035] (“queried meaningfully and efficiently”).
- HIPAA compliant. Ex1006, [0027]; see Ex1014, 93:16-95:22 (Patent Owner's expert confirming).

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Settimi

FIG. 2



Ground 2 - Evenhaim and Settimi (Claims 1-19)

Settimi's Tokens

- Settimi uses patient identifiers (PIDs) which are “encoded as part of the de-identification process to create [] encoded patient identifier[s] (EPID[s]).” EX1006, [0038].
- The EPIDs may be formed using a *hash* (as in Evenhaim). EX1006, [0041].
 - A hash is an irreversible tokenization. Ex. 1014, 37:8-38:9; 53:18-54:20; POR, 7.
- Records for the same patient, from different sources, can be identified based on their “unique identifier.” EX1006, [0037], [0040].

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Patent Owner Incorrectly Alleges that “Settimi’s queries necessarily ... rely upon patient characteristics” rather than patients. POR, 37.

- Evenhaim already teaches (and is relied upon for) searching for specific patients. EX1005, 8:18-22.
- Patent Owner’s expert agrees that a POSA would have understood that a medical database would not be limited to one type of query. Ex1014, 47:12-50:15; EX1006, [0061] (“a user may codify additional term(s) and/or create additional rules/search algorithms dynamically”).
- Settimi:
 - “[T]he user may search by the EPID.” EX1006, [0047], [0037] (“ability to connect all records relating to a single patient in the data warehouse 210” is achieved by the “unique identifier”).

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Evenhaim does not “teach[] away” from “search[ing] on anything but original micro-level data.” POR, 34.

- Preferences are not exclusions. *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009).
- Evenhaim’s preference is for “high resolution” data that allows ***patient searching***. EX1005, 7:46-58, 16:46-17:3 (explaining that low resolution data sets do “not provide the capability to aggregate ... patients by a pre-defined list of consumers”), 3:32-41.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

Evenhaim does not “teach[] away” from “search[ing] on anything but original micro-level data.” POR, 34.

- Evenhaim acknowledges that **original** name searching is not necessary. “[T]he aggregator may accept a query that includes lots of identity specifics (e.g. a list of names or a combination of a few fields that together can allow identification)—the type of query that one does not expect to be answerable in any privacy preserving fashion. This sub-step essentially converts a model base postulate about the data (that relationships that the user wonders) into a formal language query phrases according to shared variable definitions mutually accepted by the aggregator and the source-entities. ... [T]he parameter list may even include specific individuals **by name or ID or the like[]**.” EX1005, 8:30-43, 10:29-32 (“identity-free micro-data”).

Ground 2 - Evenhaim and Settimi (Claims 1-19)

The Evenhaim-Settimi Combination Does Not Violate HIPAA

- Evenhaim and Settimi are intended to **comply** with HIPAA. EX1014, 33:12-34:4; EX1005, 2:5-26.
- Patent Owner's bad actor theory.
 - Simply theorizes a potential "plain text" attack, the defenses for which Patent Owner's expert acknowledges have been known for decades. EX1014, 25:13-28:17 ("A POSA would understand that it would apply known known security techniques"), 42:10-47:11, 45:6-46:1; EX1015, ¶¶ 14-15.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

The Evenhaim-Settimi Combination Does Not Violate HIPAA

- HIPAA options
 - Statistical de-identification. EX2006, 45 C.F.R. 164.514(b)(1) (“generally accepted statistical and scientific principles and methods for rendering information not individually identifiable”; “risk is very small”).
 - Safe Harbor. EX2006; EX1016, 9-11 (“safe harbor”); EX1014, 101:12-10:2.
 - Business Associates. EX1021 (defining business associate), EX1020, 3; EX1016, 6; EX1014, 29:13-30:10 (Patent Owner’s expert explaining that one would use “a contractual agreement ... that the point of this encryption server is that it should not be sharing all of its information with the public”).
 - Re-Identification. EX2006, 45 C.F.R. 164.514(c); EX1016, 11-12.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

The Evenhaim-Settimi Combination Does Not Violate HIPAA

- Known defenses to attacks.
 - Salts and cypher block chaining. EX1014, 45:6-46:1; Ex. 1015, ¶¶ 14-15.
 - Additional levels of encryption. EX2001, ¶ 111; EX1024, 2:20-51.
 - Trusted broker/escrow agent.
 - Various compliance options articulated in HIPAA.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

The Evenhaim-Settimi Combination Does Not Violate HIPAA

- Additional Levels of Encryption
 - Patent Owner argues that Petitioner's expert does not provide corroboration. POR, 25-26 (citing EX2001, ¶ 111 (among others)).
 - Patent Owner's expert:
 - “Dr. Clark refers to an alleged ‘*additional* level of security’ that could be ‘added to the token matching system’ to provide ‘a second level of protection.’ ... Specifically, Dr. Clark states: ‘the **tokens in the patient records could be further de-identified with a second encryption key that is only available to the data source**. This allows for records belonging to the same patient to be matched for further analysis on the encryption server, but still prevents any reverse engineering of the identity back to the tokens.’ EX1003, ¶ 42.” EX2001, ¶ 111.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

The Evenhaim-Settimi Combination Does Not Violate HIPAA

- Patent Owner's expert alleges:
 - “The second level of protection that Dr. Clark refers to here ... highlights that additional ‘fixes’ would be required if token matching were to be performed at the data source entities.” EX2001, ¶ 111.
- But Petitioner's expert's explains options were well known:
 - “[M]y Prior Declaration identified another way to guard against a plain text attack. EX1003, ¶ 42. Specifically, the centralized database could simply add another level of encryption to the token before returning search results. This concept of using multiple layers of encryption would have been known to a POSA before the '641 patent, and the concept is generally described in described U.S. Pat. No. 7,668,820. EX1024, 2:20-51, 5:26-61.” EX1015, ¶ 15.
 - Ex1024, 2:20-51 (“vendor-specific key and a common longitudinal key”).

Ground 2 - Evenhaim and Settimi (Claims 1-19)

The Evenhaim-Settimi Combination Does Not Violate HIPAA

- Escrow agent or trusted broker
 - Evenhaim describes using a “trusted third party such as an escrow agent” on the aggregator side so that the encryption key **may be kept private**. EX1005, 12:63-66; *see also* EX1008, 4:9-19 (“trusted broker”).

Q Could the escrow hold keys for encryption and decryption or both? And I'm speaking generally.

A Oh, there's nothing about escrow agents that prevents them from holding different types of keys in general.

EX1014, 51:17-52:12.

Ground 2 - Evenhaim and Settimi (Claims 1-19)

The Evenhaim-Settimi Combination Does Not Violate HIPAA

- Escrow agent or trusted broker

Q What's your understanding of a trusted third party?

A It's a party that's not one of the participants in the protocol itself. It's trusted by the participants to behave properly and competently.

Q And that would include maintaining confidential information perhaps?

A That is one way you could use a trusted third party.

EX1014, 52:12-53:17.

Ground 1 - Evenhaim (Claims 1-19)

Evenhaim Describes Encrypting Individual Identifiers (Tokenization)

- “[P]erson[al] identity information ... is replaced with a unique encryption key, such as a one way hash or Advanced Encryption Standard [] or the like[.]” EX1005, 12:36-47.

Evenhaim’s Aggregator Can Perform Identifier Encryption

- “[T]here are numerous locations where an encryption of *individual identification* ... could be facilitated. ... [including] on the ‘aggregator’ processor side.” EX1005, 12:24-34.

Evenhaim Distinguishes List vs. Transmission Encryption

- Data transmission: “transmitting of data ... may preferably include respective encryption and decryption.” EX1005, 13:33-43.
- Parameter list: “regardless of the general level of encryption elected, a parameter list including ‘individuals’ should carry a stronger level of encryption.” EX1005, 14:3-13.

Ground 1 - Evenhaim (Claims 1-19)

Patent Owner's Expert Acknowledges Evenhaim's "Super Encryption"

- Patent Owner's expert admitted that the parameter list encryption described in Evenhaim differs from transmission encryption and would remain **after** the decryption of transmission encryption.
 - "The transmission encryption is peeled off, but **the super encryption remains.**" EX1014, 74:14-79:3.
- "[A]ll or part of the parameter list is encrypted." EX1005, 8:43-48.
 - Patent Owner's expert: "So I think **this language is very broad** and it could mean that **certain types of *fields* aren't encrypted and others are.**" EX1014, 74:14-79:3.
 - "[P]arameter list may even include specific individuals by name or ID or the like[]." EX1005, 8:30-43.

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Dick

- “An illustrative method ... compris[es]: receiving a request for medical information including identification of a subject ...; transmitting a query to a medical information repository for information pursuant to the request; and receiving a response to the query containing medical information.” EX1007, [0011].
- “Each request for medical information includes identification of a subject A subject might consist of a human individual or group of humans. The subject is the target of the search for medical information. The identification of the subject could be by way of name, patient number, ... or any other identification.” EX1007, [0024], [0025] (“The request may originate with insurance agencies.”).

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Dick

- “In order to legally distribute such information, a medical information repository would have to remove all ‘Identifying’ information.” EX1007, [0045].
- “The present invention contemplates the use of ‘de-identifying’ methods and processes for allowing information from the present invention to be distributed” EX1007, [0046].

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Landi

- “[S]ystems and methods that implement **secured key encryption for de-identifying patient data** to ensure patient privacy, while allowing only the owners of the patient data and/or legally empowered entities to re-identify subject patients.” EX1008, 2:30-53 (“encrypted ID”).
- “An **Encrypted ID of a given patient is a unique reproducible encrypted version of patient identifying information** that is sufficient to uniquely identify the patient.” EX1008, 5:13-36 (“store each Encrypted ID with or within a corresponding de-identified data patient data record”).
- “[C]entral patient data processing system (30) comprises **a repository of persistently stored de-identified patient data records** (35) containing de-identified (encrypted) patient identifying information ... collected from [] different clinical sites.” EX1008, 7:3-10.

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Combination of Dick and Landi

- While Dick “contemplates the use of ‘de-identifying’ methods and processes” (EX1007, [0011]), Landi sets forth a specific system for de-identification using encrypted tokens. Pet., 52.
- Both use centralized data repositories. Pet., 52-53; EX1007, [0011] (“medical information repository”); EX1008, 4:11-28 (“central patient data processing system (30)”).
- Landi describes that the de-identification occurs through encryption, where the healthcare organizations control the keys to avoid “HIPAA issues.” EX1008, 8:38-55, 10:52-63 (“[i]n accordance with HIPAA regulations”).

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Patent Owner's Arguments

- Whether there would be motivation to combine Dick and Landi because Dick (purportedly) already teaches de-identification.
- Whether Landi's de-identification to comply with HIPAA would be understood to comply with HIPAA.
- Whether the claims require “irreversibl[e] deidentification” (Sur-Reply, 22) that precludes the existence of any decryption key.

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Dick Invites De-Identification Methods

- Dick references de-identification without detailing specific technical options.
 - “The present invention further contemplates the use of ‘de-identifying’ methods and processes De-identified information comprises information that is void of any identifying information ... as understood by one ordinarily skilled in the art.” EX1007, [0013], [0046]-[0047].
 - Patent Owner admits that the issue at hand is not “mere ... ‘de-identification’.” POR, 60.

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Landi Provides a Specific De-Identification Method

- Landi details the use of encrypted IDs.
 - This “process preserves patient uniqueness to enable [] the same patient to be recognized at different collection times. In other words, this process ensures that if data is collected more than once from a particular patient, the patient will be mapped to the same Encrypted ID.” EX1008, 11:23-29.

Ground 3 – Dick and Landi (Claims 7-10 and 13)

Landi Offers Its Methods to Comply with HIPAA

- “[N]o HIPAA issues.” EX1008, 3:52-57.
- “In accordance with HIPAA.” EX1008, 10:52-63.
- Patent Owner’s expert could not say whether Landi’s methods violated HIPAA.
 - “I would need to review this in the context of HIPAA. ... I need to look at that and research it, I can’t answer that off the top of my head.” EX1014, 34:5-37:7.
 - “HIPAA compliance is – is something that takes weeks of work and analysis.” EX1014, 115:15-117:15.

Ground 3 – Dick and Landi (Claims 7-10 and 13)

HIPAA Offers Numerous Options for Compliance

- Statistical de-identification (164.514(b)(1) (“generally accepted statistical and scientific principles and methods for rendering information not individually identifiable” such that the “risk is very small”)).
- Safe harbor (164.514(b)(2)).
- Business associates (Ex1021 (defining business associate); Ex1020, 3; Ex1016, 6).
- Re-identification is permitted (164.514(c)).

Ground 3 – Dick and Landi (Claims 7-10 and 13)

The Claims Do Not Recite Irreversible De-Identification

- Claim Construction:
 - Token: “An identifier associated with an individual that does not reveal the identity of the individual.” Pet., 8.
- The ’641 Patent states that:
 - tokenization “may include encrypting respective data that identifies each individual.” EX1001, 2:37-42.

Ground 4 – Dick, Landi, and Murphy (Claims 1-6, 11, 12, and 14-19)

Murphy

- Murphy is directed to preventing targeted attacks on a “clinical data warehouse,” which attack could lead to identification of a particular patient. EX1009, 552-53 (“a system that complies with HIPAA’s ... de-identification”).
- “An attack on the system would occur by someone entering criteria into the query tool that would result in only one matching person.” EX1009, 552.
- Murphy describes the use of obfuscation to prevent the identification of a particular patient through narrowing parameters, wherein, e.g., rather than answer a query that would specify less than three patients, the systems responds with “<3”. EX1009, 555.

Ground 4 – Dick, Landi, and Murphy (Claims 1-6, 11, 12, and 14-19)

Patent Owner's Arguments

- Whether Murphy's "<3" response in lieu of giving the specific answer means "the query is still answered." POR, 66-67.
- Whether Murphy is limited to only returning a number of matching patients rather than healthcare data. POR, 68.
- Whether Murphy rejects de-identification. POR, 68.
- Whether Murphy suggests blocking queries. POR, 66-67.

Ground 4 – Dick, Landi, and Murphy (Claims 1-6, 11, 12, and 14-19)

Murphy

- Murphy's example "<3" (or some other minimum) **does not answer a query that asks for a specific number of patients**. Ex1009, 556 ("obfuscation method"); Ex1003, ¶66.
- Patent Owner's admissions support this position.
 - "[S]o that one can't see what the actual values are." EX1014, 134:8-137:16.
 - "[R]ather than returning an absolute value." POR, 67.
- Murphy is **not limited to its example query for the number of patients** meeting certain criteria. EX1009, 556 ("does not limit the logic of the query").
 - Patent Owner's expert agreed: "those examples are not limiting, it could be other things, too." EX1014, 137:17-138:22.

Ground 4 – Dick, Landi, and Murphy (Claims 1-6, 11, 12, and 14-19)

Murphy

- Murphy's does not reject de-identification.
 - Murphy calls de-identification a “good start.” EX1009, 553 (stating that even with de-identification “there is still no guarantee that someone cannot be identified in the database”).
 - Murphy states that its design removes “reservations about including increasingly patient specific data.” EX1009, 556.
- Murphy's design uses minimums to prevent attacks that “would occur by someone entering criteria into the query tool that would result in only one matching person.” EX1009, 552 (“imperative that a single individual could not be identified through the user interface”).

A decorative pattern of diagonal lines in a light blue color, running from the top-left corner towards the bottom-right, covering the left side of the page.

© 2025 Venable LLP.

This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.

VENABLE_{LLP}